AIX-EN-PROVENCE - CENTRE DES CONGRES
CULTURE NUM
JEUDI 3 JUILLET 10H-18H
en savoir plus

07 JUIL

gateGhost : traque-moi si tu peux

Applications Publié le 7/07/2014

gateGhost est un logiciel proxy anti-traqueur de publicité qui prévient les risques de tracking sur l'intégralité d'un réseau. Il fonctionne comme plugin de gatejs et est distribué sous licence GPL v3.

Il est basé sur un système de détection de traqueurs qui fonctionne avec une base de données CSV. Celui-ci permet de bloquer lesdits traqueurs soit par une fermeture de connexion, soit avec un code d'erreur 403. Il est aussi possible d'ajouter d'autres bases de données.

- Gateghost
- gatejs

Mode de fonctionnement

Les cookies

Le système d'inspection de cookie permet d'éliminer ceux qui n'ont pas été envoyés par le site consulté, ceux qui sont hors de son contrôle. Là aussi, il y a une base de données de noms de cookie à éviter. Le cookie de l'utilisateur est modifié puis forgé avant d'être renvoyé au serveur. Nous n'avons pas constaté d'impact sur la navigation en utilisant cette technique.

Le Referer

L'entête *Referer* trahit aussi nos mouvements sur la toile, il indique au site consulté d'où provient précisément la requête (le lien source).

L'utilisation de cet entête est tout à fait normale et même importante. Cependant, dans certains cas, il n'est pas souhaitable d'envoyer cette information.

gateGhost enlèvera systématiquement les Referer d'une requête quand le domaine n'est pas estimé comme proche.

En outre, une requête vers ads.tracker.com mais provenant de www.example.com ne sera pas considérée comme de confiance puisque tracker.com ne correspond pas à example.com. Dans ce cas, l'entête Referer est supprimée.

Etag

Une autre technique, plus rare, consiste à faire passer des mouchards par l'entête ETag. Une petite recherche "tracking without cookie" vous permettra de comprendre le mécanisme.

En tout état de cause, et parce que le ETag ne sert plus réellement aux systèmes de cache, l'entête est systématiquement supprimé de la réponse du serveur. Cette option est activée par défaut.

Tout est activable et désactivable à volonté.

Le SSL

Côté inconvénient, gateGhost peut poser problème quand une application, en général pour smartphones, fait du « certificat pinning », c'est-à-dire que le CA de confiance est hardcodé dans l'application. Cela empêche l'interception SSL sans erreur par l'installation d'un CA de confiance.

J'ai encore pas mal de choses à ajouter au projet telles que l'interception « propre » du SSL et la détection d'envoi de données de géolocalisation. Je précise que les contributions sont ouvertes.

Il faut aussi savoir que gateGhost est complémentaire à l'utilisation d'ads blockers ou anti-tracker installés comme greffons sur le navigateur (tel que adblocks ou ghostery), sauf que ces derniers ne s'installent pas sur un réseau et ne protègent donc pas les smartphones. Aussi, gateGhost exécute plus vite les règles via un gestionnaire spécial de mémoire associative disponible dans gatejs sous le nom de NREG.

En tout état de cause le job est fait, et ce, de manière très performante.

Points clefs

- Conçu pour les grosses architectures
- 1900 traqueurs enregistrés dans la base de données avec un système de recherche rapide
- Système d'inspection des cookies avec jusqu'à 100 noms de cookie connus
- Système de confiance sur l'entête Referer qui est enlevé quand il est non-voulu
- Technique de blocage du "tracking without cookie" basée sur l'entête HTTP - ETag
- Possibilité d'ajouter vos traqueurs

Merci à Michael Vergoz

RECHERCHER SUR LE SITE :

SUIVEZ TOOLINUX SUR TWITTER

Linux de nouveau à Metz !
Formations :
LPIC 101, 16 au 20 juin 2014
LPIC 102, 23 au 27 juin 2014
Certification 27 juin 2014
plus d'infos...
LINAGORA
en collaboration avec l'association GOALL

PARTENAIRES

- Centre Juridique Open Source
- Cedric GODART
- Planet Linagora
- Framablog
- Philippe Scoffoni
- UbuntUser
- IT-Connect
- JusteGeek

- Pour en savoir plus sur TOOLinux ou contacter la rédaction

PARTAGER CET ARTICLE :

Vous souhaitez reproduire cet article ?

A propos de TOOLinux.com | Contactez-nous | CNIL/Vie privée | Conditions de reproduction d'un article | **Groupe Linagora**

© **Copyright 2000-2014** TooLinux.com. Nous <3 SPIP